1/5/1 (Item 1 from file: 351) **Links**
Fulltext available through: Order File History
Derwent WPI

0013085361 & & *Drawing available*
WPI Acc no: 2003-165974/200316
XRPX Acc No: N2003-131071
Electronic system for authorizing cell phone user, compares and determines whether input voice of user corresponds with password selected from memory, to accordingly authorize user
Patent Assignee: NEC CORP (NIDE)
Inventor: ODA T

Patent Family (5 patents, 4 & countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20020152070	A1	20021017	US 2002117198	A	20020408	200316	B
JP 2002312318	A	20021025	JP 2001115910	A	20010413	200316	E
GB 2378297	A	20030205	GB 20028276	A	20020410	200319	E
CN 1382005	A	20021127	CN 2002122197	A	20020413	200322	E
GB 2378297	B	20030716	GB 20028276	A	20020410	200355	E

Priority Applications (no., kind, date): JP 2001115910 A 20010413

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
US 20020152070	A1	EN	17	7		
JP 2002312318	A	JA	12			

Alerting Abstract US A1
NOVELTY - A memory (7) stores keywords (71) and passwords (72) corresponding to each other. A keyboard (5) selects any arbitrary pair of keyword and password from memory. A display unit (6) displays selected keyword. A controller (1) compares and determines whether input voice of user corresponds with the selected password, to accordingly authorize a user.
DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

1. Authorized user identification program; and
2. Authorized user identification method.

USE - For authorizing user of cell phone.
ADVANTAGE - Identifies an authorized user through an easy and simple procedure and securely keeps the identification process regardless of whether the voice recognition concerns with the identification of the user or not.
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the constitution of a conventional communication system.
1 Controller
5 Keyboard
6 Display unit
7 Memory
71 Keyword
72 Password

Title Terms /Index Terms/Additional Words: ELECTRONIC; SYSTEM; AUTHORISE; CELL; TELEPHONE; USER; COMPARE; DETERMINE; INPUT; VOICE; CORRESPOND; PASSWORD; SELECT; MEMORY; ACCORD

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-0001/00	A	I	F	R	20060101

G06F-0021/20	A	I	L	R	20060101
G07C-0009/00	A	I		R	20060101
G10L-0015/00	A	I	L	R	20060101
G10L-0015/28	A	I	L	R	20060101
G10L-0017/00	A	I		R	20060101
H04M-0001/00	A	I	L	R	20060101
H04M-0001/27	A	N		R	20060101
H04M-0001/57	A	I	L	R	20060101
H04M-0001/66	A	I		R	20060101
H04M-0001/667	A	I	L	R	20060101
H04M-0001/725	A	I	L	R	20060101
G06F-0001/00	C	I	F	R	20060101
G06F-0021/20	C	I	L	R	20060101
G07C-0009/00	C	I		R	20060101
G10L-0015/00	C	I	L	R	20060101
G10L-0017/00	C	I		R	20060101
H04M-0001/00	C	I	L	R	20060101
H04M-0001/27	C	N		R	20060101
H04M-0001/57	C	I	L	R	20060101
H04M-0001/66	C	I		R	20060101
H04M-0001/72	C	I	L	R	20060101

ECLA: G07C-009/00C2D, G10L-017/00B22, H04M-001/66
ICO: T04M-001:27A
US Classification, Current Main: 704-246000; Secondary: 704-E17015
US Classification, Issued: 704246

File Segment: EngPI; EPI;
DWPI Class: T01; W01; W02; W04; P86
Manual Codes (EPI/S-X): T01-C08A; T01-J18; T01-N02B1B; T01-S03; W01-A05B; W01-C01D3C; W02-C03C1; W04-V04

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312318
（P2002－312318A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
1/00	３７０	1/00	３７０Ｅ	５Ｄ０１５
Ｇ１０Ｌ　15/00		Ｈ０４Ｍ　1/00	Ｒ	５Ｋ０２７
15/28		1/57		５Ｋ０３６
17/00		1/667		

審査請求　未請求　請求項の数19　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2001－115910(P2001－115910)

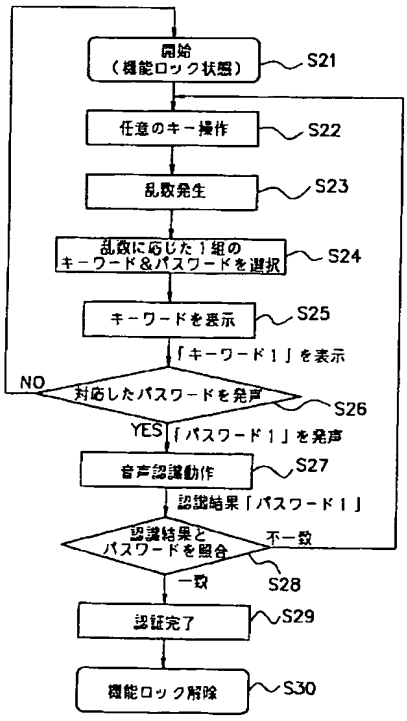
(22)出願日　平成13年４月13日(2001.4.13)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　小田　利明
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100084250
弁理士　丸山　隆夫

最終頁に続く

(54)【発明の名称】　電子装置、本人認証方法およびプログラム

(57)【要約】
【課題】　入力音声を認識して端末ユーザ本人の認証を行う携帯電話端末および本人認証方法を提供する。
【解決手段】　あらかじめ登録された複数組のキーワードとパスワードの中からランダムに選択した１組のペアのキーワードを表示部に表示し、その表示を見たユーザに、キーワードとペアとなるパスワードを発声させる。そして、その発声の音声認識結果をもとに、ユーザから発声されたパスワードと表示したキーワードと対になるパスワードとの同一性を照合して、端末使用者本人の認証を行う。



1

【特許請求の範囲】

【請求項１】　音声認識手段を有する電子装置において、

１対１に対応する１あるいはそれ以上のキーワードとパスワードの組を登録する手段と、

前記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択する選択手段と、

前記選択したキーワードを表示する表示手段と、

前記音声認識手段によって、当該電子装置外部からの音声を認識する手段と、

前記認識結果をもとに、前記音声と、前記表示したキーワードと組になるパスワードとが一致するかどうかの照合処理をする手段とを備え、

前記照合処理の結果、前記音声とパスワードとが一致した場合、その音声の発声者を当該電子装置の使用者本人であると認証することを特徴とする電子装置。

【請求項２】　前記選択手段は、前記登録されたキーワードとパスワードの組より任意の１組、あるいは複数組のキーワードとパスワードを選択することを特徴とする請求項１記載の電子装置。

【請求項３】　さらに、乱数を発生する手段を備え、前記選択手段は、その乱数に従って、前記任意の１組、あるいは複数組のキーワードとパスワードを選択することを特徴とする請求項２記載の電子装置。

【請求項４】　前記選択した複数組のキーワードとパスワードの全てのキーワードに対して前記照合処理を行うことを特徴とする請求項３記載の電子装置。

【請求項５】　前記照合処理において、前記複数組のキーワードとパスワードの全てのキーワードについて前記音声とパスワードとが一致した場合に、その音声の発声者を当該電子装置の使用者本人であると認証することを特徴とする請求項４記載の電子装置。

【請求項６】　前記照合処理において、前記複数組のキーワードとパスワードに係るキーワードの内、一定数以上のキーワードについて前記音声とパスワードとが一致した場合に、その音声の発声者を当該電子装置の使用者本人であると認証することを特徴とする請求項４記載の電子装置。

【請求項７】　前記表示手段は、前記キーワードを可視表示および／または可聴表示することを特徴とする請求項１記載の電子装置。

【請求項８】　前記音声認識手段は、不特定の話者についての不特定音声認識を行うことを特徴とする請求項１記載の電子装置。

【請求項９】　前記音声認識手段は、特定の話者についての特定音声認識を行うことを特徴とする請求項１記載の電子装置。

【請求項１０】　前記音声認識手段は、前記選択された複数組のキーワードとパスワードの内、特定のキーワードについて前記特定音声認識を行い、他のキーワードについて前記不特定音声認識を行うことを特徴とする請求項８または９に記載の電子装置。

2

【請求項１１】　前記電子装置は、携帯電話端末であることを特徴とする請求項１乃至１０のいずれかに記載の電子装置。

【請求項１２】　音声認識機能を有する電子装置における本人認証方法であって、

１対１に対応する１あるいはそれ以上のキーワードとパスワードを登録するステップと、

前記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択するステップと、

前記選択したキーワードを表示するステップと、

前記音声認識機能によって、前記電子装置外部からの音声を認識するステップと、

前記認識ステップで得た結果をもとに、前記音声と、前記表示したキーワードと組になるパスワードとが一致するかどうかの照合を行うステップと、

前記照合ステップにおいて、前記音声とパスワードとが一致するとの照合結果が得られた場合、その音声の発声者を前記電子装置の使用者本人であると認証するステップとを備えることを特徴とする本人認証方法。

【請求項１３】　前記選択ステップは、前記登録されたキーワードとパスワードの組より任意の１組、あるいは複数組のキーワードとパスワードを選択することを特徴とする請求項１２記載の本人認証方法。

【請求項１４】　さらに、乱数を発生するステップを備え、前記選択ステップでは、その乱数に従って、前記任意の１組、あるいは複数組のキーワードとパスワードを選択することを特徴とする請求項１３記載の本人認証方法。

【請求項１５】　前記照合ステップは、前記選択した複数組のキーワードとパスワードの全てのキーワードに対して前記照合を行うことを特徴とする請求項１４記載の本人認証方法。

【請求項１６】　前記認証ステップは、前記複数組のキーワードとパスワードの全てのキーワードについて前記音声とパスワードとが一致した場合に、その音声の発声者を前記電子装置の使用者本人であると認証することを特徴とする請求項１５記載の本人認証方法。

【請求項１７】　前記認証ステップは、前記複数組のキーワードとパスワードに係る全てのキーワードの内、一定数以上のキーワードについて前記音声とパスワードとが一致した場合に、その音声の発声者を前記電子装置の使用者本人であると認証することを特徴とする請求項１５記載の本人認証方法。

【請求項１８】　前記選択された複数組のキーワードとパスワードの内、特定のキーワードについて前記音声認識機能による特定音声認識を行い、他のキーワードについて前記音声認識機能による不特定音声認識を行うことを特徴とする請求項１７記載の本人認証方法。

【請求項１９】　音声認識機能を有する電子装置において本人を認証するために用いるプログラムであって、
１対１に対応する１あるいはそれ以上のキーワードとパスワードを登録する処理と、
前記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択する処理と、
前記選択したキーワードを表示する処理と、
前記音声認識機能によって、前記電子装置外部から入力された音声を認識する処理と、
前記認識処理で得た結果をもとに、前記音声と、前記表示したキーワードと組になるパスワードとが一致するかどうかの照合を行う処理と、
前記照合処理における結果が、前記音声とパスワードとの一致を示している場合、その音声の発声者を前記電子装置の使用者本人であると認証する処理とを実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音声認識機能を使用して本人を認証する電子装置、本人認証方法およびプログラムに関するものである。

【０００２】

【従来の技術】近年における携帯電話端末の普及の拡大により、紛失、あるいは盗難による端末の不正使用や個人情報（プライバシー）の漏洩等が懸念され始めている。このような、端末の不正使用等を防止するため、現行の機種では、ユーザが端末のキーを使用して、あらかじめ設定されたパスワードを入力することにより、本人の認証を可能としているものがある。

【０００３】端末の不正使用等を防止するため、既に提案されている技術としては、例えば、特開平９－８４１２８号公報に記載の通信機器や、特開平８－８４１９０号公報に記載の不正使用防止装置がある。これらの内、特開平９－８４１２８号公報は、音声認識機能を有する通信機器において、その機器を使用して通話中の者の音声をパラメータ化し、それを、あらかじめ記憶したパラメータと比較することで、その者が正規の使用者かどうかを判断する技術を開示している。

【０００４】特開平８－８４１９０号公報に記載の不正使用防止装置は、あらかじめ個人認識用の複数の暗号音声データ、あるいは声紋データを、認証用データベースとして記憶しておき、そのデータベースから選択指定した特定のキーワードを話者に発声させて、その音声入力と上記の暗号音声データ、あるいは声紋データとを照合する。そして、その照合ができない場合に、認証信号の不正使用が発生したと判定する。

【０００５】図７は、従来の通信機器の構成例を示すブロック図である。同図に示す機器は、キーボード７０６から入力された暗証番号と、事前に登録された暗証番号との比較を行い、それらが一致すれば、ダイヤルロックを解除して、その通信機器を受信待ち受け、およびダイヤル発呼状態にする。

【０００６】一方、メモリ７１０には、あらかじめ、正規の機器使用者の音声符号化パラメータが登録されている。また、音声パラメータ比較回路７１１は、上記の暗証番号比較処理の後に、通話状態中の話者の音声符号化パラメータを求める。そして、求めたパラメータと、上記のメモリ７１０に記憶されたパラメータとを比較し、一定時間内に両パラメータの一致を判定できない場合には、回線を切断する。

【０００７】

【発明が解決しようとする課題】しかしながら、上記従来の技術には、以下のような問題がある。例えば、現行機種において一般的となっている、端末から入力されたキー情報（パスワード）をもとに本人の認証を行う方式では、ユーザは煩雑な操作をする必要があり、しかも、ユーザに対して、複数桁の数字のキー入力を強要することが不可避である、という問題がある。

【０００８】また、キー入力を容易にするため、文字数の少ないパスワードを採用したとしても、その少文字数化のためにパスワードが他人に解読されやすくなり、不正使用を十分に防止できないという問題も発生する。

【０００９】一方、上述した特開平９－８４１２８号公報、特開平８－８４１９０号公報に記載の技術は、いずれも、不正使用の防止のため、あらかじめユーザ（話者）による音声情報（特開平８－８４１９０号では、個人認証用の暗号音声データ、声紋データ、また、特開平９－８４１２８号では、使用者の音声符号化パラメータ）の登録が必須である。そして、その登録のため、ユーザに与える負担、煩雑さがあるばかりでなく、データ量が膨大となる、音声による個人認識情報の事前登録を要する方式そのものが、装置の複雑化、大規模化を招くという問題がある。

【００１０】本発明は、上述の課題に鑑みなてされたものであり、その目的とするところは、入力された音声をもとに、端末ユーザ本人であることの認証を、秘匿性を保持しながら行うことのできる電子装置および本人認証方法を提供することである。

【００１１】本発明の他の目的は、話者を特定した音声認識処理、あるいは話者を特定しない音声認識処理のいずれにおいても高い秘匿性を持ち、容易かつ簡単な構成で本人の認証を行うことのできる電子装置および本人認証方法を提供することである。

【００１２】

【課題を解決するための手段】上記の目的を達成するため、本発明に係る電子装置は、１対１に対応する１あるいはそれ以上のキーワードとパスワードの組を登録する手段と、上記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択する選択手段と、上記選択したキーワードを表示する表示手段と、

上記音声認識手段によって、当該電子装置外部からの音声を認識する手段と、上記認識結果をもとに、上記音声と、上記表示したキーワードと組になるパスワードとが一致するかどうかの照合処理をする手段とを備え、上記照合処理の結果、上記音声とパスワードとが一致した場合、その音声の発声者を当該電子装置の使用者本人であると認証する。

【００１３】好ましくは、上記選択手段は、上記登録されたキーワードとパスワードの組より任意の１組、あるいは複数組のキーワードとパスワードを選択する。

【００１４】好適には、本発明に係る電子装置は、さらに、乱数を発生する手段を備え、上記選択手段は、その乱数に従って、上記任意の１組、あるいは複数組のキーワードとパスワードを選択する。

【００１５】さらに、好適には、上記音声認識手段は、上記選択された複数組のキーワードとパスワードの内、特定のキーワードについて上記特定音声認識を行い、他のキーワードについて上記不特定音声認識を行う。

【００１６】また、他の発明は、音声認識機能を有する電子装置における本人認証方法であって、１対１に対応する１あるいはそれ以上のキーワードとパスワードを登録するステップと、上記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択するステップと、上記選択したキーワードを表示するステップと、上記音声認識機能によって、上記電子装置外部からの音声を認識するステップと、上記認識ステップで得た結果をもとに、上記音声と、上記表示したキーワードと組になるパスワードとが一致するかどうかの照合を行うステップと、上記照合ステップにおいて、上記音声とパスワードとが一致するとの照合結果が得られた場合、その音声の発声者を上記電子装置の使用者本人であると認証するステップとを備える。

【００１７】好適には、上記選択ステップは、上記登録されたキーワードとパスワードの組より任意の１組、あるいは複数組のキーワードとパスワードを選択する。

【００１８】また、好適には、他の発明に係る本人認証方法は、さらに、乱数を発生するステップを備え、上記選択ステップでは、その乱数に従って、上記任意の１組、あるいは複数組のキーワードとパスワードを選択する。

【００１９】さらに、他の発明は、音声認識機能を有する電子装置において本人を認証するために用いるプログラムであって、１対１に対応する１あるいはそれ以上のキーワードとパスワードを登録する処理と、上記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択する処理と、上記選択したキーワードを表示する処理と、上記音声認識機能によって、上記電子装置外部から入力された音声を認識する処理と、上記認識処理で得た結果をもとに、上記音声と、上記表示したキーワードと組になるパスワードとが一致するかどうかの照合を行う処理と、上記照合処理における結果が、上記音声とパスワードとの一致を示している場合、その音声の発声者を上記電子装置の使用者本人であると認証する処理とを実行させるためのプログラムを提供する。

【００２０】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を詳細に説明する。なお、以下の各実施の形態においては、電子装置として携帯電話端末を例にとって、その動作等を説明する。

【００２１】［実施の形態１］図１は、本発明の実施の形態１に係る携帯電話端末の主要部の構成を示すブロック図である。同図に示す携帯電話端末（以降、適宜、端末ともいう）において、制御部１は、本携帯電話端末全体を制御する、例えば、マイクロプロセッサからなる中央制御装置（ＣＰＵ）であり、必要に応じて、後述する各構成部にアクセス等をする。

【００２２】マイク２は、本端末の外部から入力された音声を電気信号に変換し、変換後の信号を音声処理部３に与える。この音声処理部３は、例えば、符号化／復号化器（ＣＯＤＥＣ）からなり、マイク２からの音声信号をディジタル信号に変換する。また、音声認識部４は、音声処理部３でディジタル信号に変換された音声データをもとに、後述する所定の音声認識動作を行う。

【００２３】キー入力部５は、端末上に配された機能キーやテンキー等（不図示）を含み、ユーザが、これらの内の任意のキーを押下したことを認識し、その結果を制御部１に通知する。また、表示部６は、制御部１からの指示に従って、任意の文字、絵等を可視表示する、例えば、液晶表示器（ＬＣＤ）で構成されている。

【００２４】記憶部７は、キーワード７１、パスワード７２、および、これらの対応関係を示す対応データ７３（これらについては、後述する）を記憶し、必要に応じて出力する。ここでは、制御部１が記憶部７にアクセスすることで、データの読み出しやデータの書き込み動作を行う。乱数発生器８は、制御部１からの指示に従って所定の乱数を発生させ、それを制御部１に通知する。

【００２５】通信部１１は、本携帯電話端末における無線通信機能を実現するため送受信部や周波数変換部等（不図示）を備えている。具体的には、アンテナ１２で受信した電波信号は、通信部１１で処理された後、制御部１へ送られ、また、マイク２からの音声信号や符号化された文字情報等が、通信部１１を介してアンテナ１２より空間へ送出される。なお、本携帯電話端末の変調方式は、本願発明の技術には直接関係しないため、ディジタル方式、アナログ方式のいずれであってもよい。

【００２６】また、後述するユーザ認証等の処理は、不図示の不揮発性メモリ（例えば、読み出し専用メモリ（ＲＯＭ））内に格納されたプログラムに従って、制御部１によって実行される。

【００２７】本実施の形態１に係る携帯電話端末は、上記のマイク２を介して入力された音声をもとに、端末のユーザが、ユーザ本人であることの認証を行うことを特徴とする。そのため、本携帯電話端末には、あらかじめ複数のキーワードと、それらに１対１で対応するパスワードとを登録しておく。

【００２８】本端末は、認証動作開始時に、あらかじめ登録されたキーワード、パスワードの組の中から、ランダムに１組のキーワードとパスワードのペアを選択し、表示部に表示したキーワードとペアとなるパスワードを、ユーザに音声で発声（通常の口頭による発音）させて、それを認識する。そして、その認識結果について、あらかじめ設定されたパスワードとの同一性を照合することにより、その発声主が本人（つまり、当該電話端末の真のユーザ）であることの認証を行う。

【００２９】なお、これら複数のキーワードとパスワードは、例えば、端末のユーザ自身があらかじめ端末内のメモリ（ここでは、記憶部７）に登録するが、その際、ユーザは、通常、自分しか知りえない、あるいはユーザ特有の発想に従って、所定の言葉（ユーザ自身が再現できる限りにおいて、その文字数は不問）を選んで登録する。従って、キーワード等は、全くの個人情報に関係するものであっても、あるいは、単なる数字や文字、簡単な単語でもよい。そして、このような登録方法をとることにより、キーワードとパスワードの相互関係等については、その秘匿性を十分に維持できる。

【００３０】そこで、本実施の形態１に係る携帯電話端末における本人の認証動作について詳細に説明する。図２は、本実施の形態１に係る携帯電話端末における、音声認識による本人認証処理の動作および処理手順を示すフローチャートである。本携帯電話端末は、その動作開始時には、端末にロックがかかった状態にあり、この状態では、ユーザは、携帯電話端末のいかなる機能をも使用することができない（図２のステップＳ２１に示す「機能ロック状態」）。

【００３１】携帯電話端末が機能ロック状態にあるとき、ユーザがその端末を使用しようとして、キー入力部５の任意のキーを押下すると、キー入力部５より制御部１に対して、キー押下があった旨の通知がなされる（ステップＳ２２）。この通知を受けた制御部１は、乱数発生器８に所定の起動信号を送り、乱数発生器８を動作させる。その結果、制御部１は、乱数発生器８より発せられた値（乱数）を入手する（ステップＳ２３）。

【００３２】次に、制御部１は、ステップＳ２４において、あらかじめ記憶部７に登録された複数組のキーワードとパスワードのペアの中から、上記の乱数の値に対応した１組、例えば、「キーワード１」と「パスワード１」を選択する。図３は、記憶部７内に登録された複数組のキーワード３１とパスワード３２のペアの中から、その１組（ここでは、「キーワード１」と「パスワード１」）を選択する様子を模式的に示す図である。

【００３３】図３に示すように、キーワード３１とパスワード３２は、１対１に対応させて記憶部７内に登録されており、制御部１は、それらの中から、乱数発生器８より得られた乱数の値に応じて、ランダムに１組のキーワードとパスワードのペアを選択する。

【００３４】このように、キーワードとパスワードのペアを選択すると、制御部１は、ステップＳ２５において、そのペアを構成するキーワード（ここでは、「キーワード１」）のみを、ユーザが認識できる文字の形態で表示部６に可視表示する。この表示は、ユーザに対して「キーワード１」に対応するパスワードの発声を促すものである。

【００３５】そこで、ステップＳ２６では、上記の「キーワード１」の表示を見たユーザから発声（具体的には、そのキーワードに対応するパスワードの発声）があったかどうかを判断する。なお、このとき、ユーザは、ユーザ自身の記憶の中から「キーワード１」とペアとなる「パスワード１」を探り出し、それを音声で発声することになる。

【００３６】ユーザからの発声があれば、それがマイク２で捕えられ、音声信号として音声処理部３に伝えられた後、ディジタル信号に変換されて、音声認識部４に入力される。音声認識部４は、このディジタル信号を受けて所定の音声認識動作を行い、ユーザから発声された音声を符号化する変換処理を実行する（ステップＳ２７）。

【００３７】なお、ステップＳ２６において、ユーザから何らの発声もないと判断されれば、本処理は最初に戻り、本携帯電話端末は、上述した「機能ロック状態」に維持されることになる。

【００３８】ステップＳ２７における音声認識動作によって符号化されたユーザの発声内容は、音声認識結果として、続くステップＳ２８において、上記のステップＳ２４で選択された「パスワード１」と一致するかどうかの照合が行われる。その結果、この音声認識結果と「パスワード１」とが一致すれば、認識された発声内容は、その端末の使用者本人からのものであることになる。そのため、ステップＳ２９において、確認（認証）を完了する。

【００３９】上記の認識処理、並びに認証完了（ステップＳ２７～Ｓ２９）の結果、真のユーザがその携帯電話端末を使用しようとしていることが判明したため、制御部１は、ステップＳ３０において、端末の機能ロックを解除し、そのユーザは、通常の状態で携帯電話端末の機能の使用が可能となる。

【００４０】しかし、ステップＳ２８の照合処理において、音声認識の結果と「パスワード１」とが不一致と判断されれば、再びステップＳ２２に戻って、任意のキー押下（キー操作）を待つ。このように処理するのは、端

末の不正使用の防止とともに、真の端末ユーザであっても、何らかの原因でパスワードを忘れたり、あるいは言い違いをする場合があることを想定したためである。

【００４１】以上説明したように、本実施の形態１によれば、あらかじめ登録された複数組のキーワードとパスワードの中からランダムに選択した１組のペアにキーワードを表示部に表示し、そのキーワードとペアとなるパスワードを、ユーザに口頭による音声で発声させて、それに対する音声認識をする。そして、その認識結果をもとに、発声されたパスワードと、表示したキーワードとペアになるパスワードとの同一性を照合するという処理を行うことにより、単純な手順で、確実に本人（ユーザ）の認証を行うことができる。

【００４２】また、既に音声認識機能が搭載されている携帯電話端末に、本認証方法を適用することで、新たなハードウエアの追加なしに、低コスト、かつ簡単な構成でユーザ認証を実現できる。

【００４３】換言すれば、本実施の形態１に係るユーザの認証方法は、近時、携帯電話端末において多く用いられるようになってきている音声認識機能をそのまま流用でき、ユーザは、本人認証のための煩雑なキー操作によるパスワード入力から解放されるとともに、現状の携帯電話端末のハードウエア、およびソフトウエアを大幅に変更することなく、本人の認証を行えるという多大な効果を奏する。

【００４４】さらには、あらかじめ登録した複数のキーワードとパスワードのペアの中から、乱数を使用してランダムに選択したキーワードに対応したパスワードを用いて認証を行うことにより、パスワードの推測が困難となり、より安全性、並びに秘匿性の高い、確実な認証機能を実現できるという効果がある。

【００４５】従って、本実施の形態に係る認証方式は、ユーザ本人の音声を使用しての個人認識情報の事前登録が不要となり、かかる登録を要する従来の方式に比べて、ユーザの負担が大幅に軽減され、しかも、認証機能のための特別な大容量メモリを端末に備える必要もなくなる。このことが、小型軽量が不可欠の要件となる携帯電話端末に対して、大きな利点をもたらす。

【００４６】［実施の形態２］以下、本発明の実施の形態２について説明する。なお、本実施の形態２に係る携帯電話端末は、図１に示す、上記実施の形態１に係る携帯電話端末と同一の構成をとるため、ここでは、その図示および説明を省略する。

【００４７】本実施の形態２に係る携帯電話端末の特徴は、ユーザの認証動作開始時に、あらかじめ登録された、１対１に対応する複数のキーワードとパスワードの組の中から、ランダムに複数組のキーワードとパスワードのペアを選択し、それらのキーワードを、順次、表示部に表示する。そして、ユーザには、表示されたキーワードとペアとなるパスワードを音声で発声させ、その認識結果について、あらかじめ設定されたパスワードとの同一性を照合して、本人の認証を行う。

【００４８】図４は、本実施の形態２に係る携帯電話端末における、音声認識による本人認証のための動作および処理手順を示すフローチャートである。本実施の形態２に係る携帯電話端末の基本動作は、上記実施の形態１に係る携帯電話端末と同様であるが、上述のように、ランダムに選択されるキーワードとパスワードのペアの数等に違いがある。

【００４９】本実施の形態２に係る携帯電話端末も、図４のステップＳ４１に示すように、その動作開始時には「機能ロック状態」にあり、ユーザは、携帯電話端末のいかなる機能をも使用することができないことは、実施の形態１に係る携帯電話端末と同様である。

【００５０】そこで、ステップＳ４２で、キー入力部５上の任意のキーが押下されると、キー入力部５より制御部１にキー押下があった旨の通知がなされる。同時に、制御部１は、後述する照合動作の回数を計数するパラメータｎを０にする（初期化）。そして、続くステップＳ４３において、ｎを１だけインクリメントする（ｎ←ｎ＋１）。

【００５１】制御部１は、上記のキー押下の通知を受けると、乱数発生器８に所定の起動信号を送り、それを動作させる。その結果、制御部１は、乱数発生器８が発生した乱数を受け取る（ステップＳ４４）。続くステップＳ４５において、制御部１は、あらかじめ記憶部７に登録された複数組のキーワードとパスワードのペアの中から、乱数発生器８より受け取った乱数の値に応じて、Ｎ組のキーワードとパスワード（例えば「キーワード１」～「キーワードＮ」と、「パスワード１」～「パスワードＮ」）を選択する。

【００５２】図５は、制御部１が、記憶部７内に登録された複数組のキーワード５１とパスワード５２のペアの中から、Ｎ組のキーワードとパスワード（ここでは、上述のように「キーワード１」～「キーワードＮ」と、「パスワード１」～「パスワードＮ」）を選択する様子を模式的に示している。

【００５３】ここでも、上記実施の形態１の場合と同様、キーワード５１とパスワード５２は、１対１に対応させて記憶部７内に登録されており、制御部１は、それらの中から、乱数発生器８より得られた乱数の値に応じてＮ組のキーワードとパスワードのペアを選択する。

【００５４】このようにキーワードとパスワードのペアを選択後、制御部１は、ステップＳ４６において、表示部５に、「キーワード１」～「キーワードＮ」の内、まず、「キーワード１」を、ユーザが認識できる文字形態で表示させる。そして、上記の実施の形態１の場合と同様に、ユーザが「キーワード１」の表示を見て、それに対応するパスワードの発声をするように促す。

【００５５】ステップＳ４７では、「キーワード１」の

表示を見たユーザから、そのキーワードに対応するパスワードの発声があったかどうかを判断する。ユーザは、ユーザ自身の記憶の中から「キーワード１」とペアとなる「パスワード１」を探り出して、それを音声で発声することは、上記実施の形態１の場合と全く同じである。

【００５６】すなわち、ユーザからの発声は、マイク２で捕えられ、それが音声信号として音声処理部３に伝えられる。そして、その信号はディジタル信号に変換された後、音声認識部４に入力される。音声認識部４は、このディジタル信号に対して所定の音声認識動作を行い、ユーザが、携帯電話端末外部よりマイク２に向けて発声した音声を符号化（変換処理）する（ステップＳ４８）。しかし、ステップＳ４７で、音声入力がない（ユーザからの発声がない）と判断された場合には、ユーザによる音声発生がないとして、本処理は最初に戻る。よって、本携帯電話端末は、「機能ロック状態」に維持される。

【００５７】続くステップＳ４９において、上記の音声認識動作によって符号化されたユーザの発声内容が、音声認識の結果として、上記のステップＳ４５で選択された「パスワード１」と一致するかどうか、その照合が行われる。かかる照合により、音声認識結果と「パスワード１」とが一致すれば、認識された発声内容は、「キーワード１」に関して、その端末のユーザ本人からのものと判断される。

【００５８】そして、ステップＳ５０で、上述したパラメータｎが、あらかじめ設定した照合動作回数と一致するかどうかを判定し、それらが一致しなければ、処理をステップＳ４３に戻して、ｎを１インクリメントする。すなわち、「キーワード１」と「パスワード１」の組に対する照合が終了すると、ｎのインクリメントによって、次の２組目の「キーワード２」と「パスワード２」に対する照合動作の準備に入る。

【００５９】ここでは、２組目の「キーワード２」と「パスワード２」に対しても、ステップＳ４３～Ｓ４９において、１組目の場合と同様の照合処理を行う。そして、それ以降、ステップＳ５０においてｎ＝Ｎとなるまで、つまり、Ｎ組目の「キーワードＮ」と「パスワードＮ」に対する照合動作が行われるまで、これらステップＳ４３～Ｓ４９の処理をＮ回、繰り返す。

【００６０】ステップＳ５０において、ｎ＝Ｎと判断されれば、１組～Ｎ組の「キーワード」と「パスワード」に対して照合動作が行われたことになるため、ステップＳ５１において、確認（認証）を完了する。言い換えれば、全ての組についての照合がなされて初めて、使用者本人であることの確認が完了する。そこで、制御部１は、ステップＳ５２において、端末の機能ロックを解除し、それ以降、携帯電話端末の機能の使用が可能な状態となる。

【００６１】なお、ステップＳ４９の照合処理において、音声認識の結果とパスワードとが不一致と判断されれば、処理をステップＳ４２に戻して、ユーザによる任意のキー操作を待つ。また、このステップＳ４２では、パラメータｎ（照合動作の回数を示す）を“０”に初期化するため、上記のごとく不一致という判断がなされた場合、照合処理は、必ず「キーワード１」に対する「パスワード１」の照合から始まることになる。

【００６２】以上説明したように、本実施の形態２によれば、複数のキーワードとパスワードの組の中から、ランダムに複数組のキーワードとパスワードのペアを選択し、それら複数組のキーワードとパスワードのペア全てについて同一性の照合処理を行うことで、１組のキーワードとパスワードのペアについて照合処理を行う場合に比べて、第三者がパスワードを解読することが、より困難となる。従って、厳密、かつ確実な上、高い秘匿性を保持したユーザ認証を行える。

【００６３】また、認証動作を行う際のキーワードとパスワードのペアとして、複数組（Ｎ組）を選択し、これらを用いて複数回（Ｎ回）の照合を行うことにより、例えば、不正照合といった行為に対して、より安全性を高く保持しつつ、高精度な、端末の使用者本人の認証機能が得られる。

【００６４】ここで、上記の実施の形態１，２で説明した、本願発明に係る本人認証のための動作と携帯電話端末の動作との関係について、具体的に説明する。図６は、携帯電話端末の一連の動作における、本願発明に係る本人認証動作の位置づけを示すフローチャートである。同図のステップＳ６１で、端末の電源がＯＮになると、続くステップＳ６２において、その端末がいわゆる「施錠」状態になっているかどうかが判定される。

【００６５】そこで、端末のユーザが、その施錠状態を解きたいと欲すれば、ステップＳ６３において、「開錠」動作を行う。上述した本願発明に係る本人認証技術は、この開錠動作に適用することができる。すなわち、ステップＳ６３で、ユーザが、提示されたキーワードとペアとなるパスワードを発声し、その音声認識結果が、キーワードとパスワードのペアの正当性を示した場合、本人認証が完了したとして、端末の「開錠」が行われる。

【００６６】その結果、端末は使用可能な状態になり（ステップＳ６４）、通話を含めて、ユーザが自由に端末を操作できる。なお、ステップＳ６２で、端末が施錠状態にないと判断された場合には、上記の開錠動作を経ずとも、ユーザは、端末を自由に使用できる。

【００６７】また、使用可能な状態にある端末を施錠状態にしたい場合（ステップＳ６５でＹＥＳ）、ユーザは、ステップＳ６６において、例えば、ボタン（テンキー等）を押下して特定のキー入力操作やパスワード入力を行う。その結果、ステップＳ６７で、その端末は使用不能状態になる。以降、必要に応じて、これらの動作や

操作が繰り返される。なお、端末の電源をＯＦＦにする動作は、図６に示す流れの中のいずれの処理においても行える。

【００６８】このように、本願発明に係る本人認証のための動作を、端末の開錠時の操作に適用することで、キーワードに対する適正なパスワードを知る本人以外は、端末の施錠状態を解けない。そのため、端末の不正使用や、端末に格納された個人情報の窃用を確実に防止できる。

【００６９】なお、本願発明に係る本人認証方法を適用する電子装置は、携帯電話端末に特化されるものではなく、他の通信装置、通信端末、電子機器等にも適用できることは言うまでもない。また、本発明は、上記の実施の形態１，２に限定されるものではなく、本発明の趣旨を逸脱しない範囲において、種々の変形が可能である。以下、上記実施の形態１，２の変形例について説明する。

【００７０】＜変形例１＞上記の実施の形態１，２では、複数のキーワードとパスワードを、端末のユーザ自身があらかじめ記憶部７に登録するようにしているが、これらの内、キーワードだけは、ユーザ以外の者、例えば、端末メーカー、販売店等が、その端末の製造時（あるいは、出荷時、販売時）に初期設定しておき、ユーザは、それら既存のキーワードに対応するパスワードを登録するだけで済むようにしてもよい。これによって、ユーザは、キーワードとパスワードの両方の登録操作をしなければならないという煩わしさから開放され、登録操作を簡素化できる。

【００７１】このとき、端末の制御部１によって、その記憶部７が、何らデータが書き込まれていない状態にあるかどうかを判断し、それがメモリ空き状態にある場合に、パスワードの登録モードに入るようにしてもよい。換言すれば、端末にキーワードが１つでも登録されていれば、上述した本人認証の動作に入り、キーワードの登録が何もなければ、当該端末を不特定の者が使用できるようにしてもよい。さらに、端末が使用可能な状態にあるとき（例えば、上述した図６のステップＳ６４の状態）、パスワードの変更や更新を行えるようにしてもよい。

【００７２】なお、記憶部７へのデータ書き込み状況に応じて、上記の登録モードへ移行するか否かを決定する点に鑑みた場合、図６に示す処理は、その端末に、既にキーワードの登録がされていることが前提となる。

【００７３】＜変形例２＞上記の実施の形態１，２では、ユーザが視認できる形で表示部６にキーワードを可視表示し、それを見たユーザが、それに対応するパスワードを発声するよう、ユーザを促す構成をとっているが、このキーワードの表示とともに、別途、端末より音声で、例えば、「ペアとなるパスワードを発声してください。」といったメッセージを出すようにしてもよい。こうすることで、端末の使用開始時における、端末操作に関するユーザの混乱が防止できる。

【００７４】また、同時に、キーワードの可視表示とともに、キーワードそのものを、例えば、端末のスピーカ等を介して可聴音で音声出力するようにしてもよい。こうすることで、特に、目が不自由である等の視覚障害を持つ人にとって利便性が向上し、よりユーザフレンドリーな携帯電話端末を提供できることになる。

【００７５】＜変形例３＞上記の実施の形態２に係る携帯電話端末では、認証処理を行う際、Ｎ組のキーワードとパスワードのペアについて、ｎ回（ｎ＝Ｎ）の照合処理を行っているが、例えば、急を要する端末の使用状況が発生した場合等に備えて、ユーザによる選択、あるいはユーザからの指定によって、Ｎ組のペアの中から、数組について音声認識動作（認証処理）を行えるように構成してもよい。かかる構成によって、ユーザ認証の確度を低下させずに、ユーザの意志によって、認証処理の自由度を向上させることができる。

【００７６】＜変形例４＞また、上記実施の形態２では、選択したＮ組のキーワードとパスワードのペアに対して、Ｎ回の照合を行い、それら全てについての認証結果とパスワードとの一致があったときに認証終了としているが、これに限定されない構成としてもよい。すなわち、正答率という発想を導入し、認証動作中において、端末のユーザが、提示されたキーワードに対して一定数以上のペア（例えば、２～３個のペア）についてパスワードを正確に発声できた場合に、所定の正答率を越えた、あるいは達成したとして、そのユーザを使用者本人であると認証するようにしてもよい。これにより、認証処理の迅速化が図れる。

【００７７】＜変形例５＞上記の実施の形態１，２では、音声認識の結果とパスワードとが不一致と判断された場合、再度、任意のキー操作を待つ処理に戻る構成をとっているが、かかる不一致の判断がなされた回数を計数して、それが一定数以上となったときには、認証処理を強制的に終了させるようにしてもよい。

【００７８】すなわち、一定回数以上、パスワードを言い違える者は、ユーザ本人ではない可能性が高いといえるため、以降において認証処理を繰り返さず、その端末を使用不能とする扱い（具体的には、上述した機能ロック状態の維持）にしても、不都合はないと考えられるからである。そして、このような構成とすることで、悪意、あるいは不正を働く意志を持って端末を使用しようとする者を容易に排除できる。

【００７９】＜変形例６＞記憶部７に登録する複数のキーワードとパスワードは、端末のユーザ自身によって何時でも更新ができる構成としてもよい。また、更新回数が増えて、ユーザ自身が、ペアとなるパスワードを忘れる可能性があるため、ユーザのみが知る特殊なキー操作によって、キーワードとパスワードを確認できる構成を

設けてもよい。さらに、パスワードの更新時にのみ、これらのキーワード等を確認できるようにしてもよい。

【００８０】また、ユーザがパスワードを忘れた場合の手当として、例えば、提示された５個のキーワードの内、４個に対して正確なパスワードを言えた場合や、提示されたものの内、例えば、２ペアについて連続して正解した場合、本人であるとの認証を行うようにしてもよい。

【００８１】＜変形例７＞上記の実施の形態１，２に係る携帯電話端末では、本人認識動作の際、その認識の対象とする音声は不特定の者が発する音声としているが、これを特定音声認識方式による認証としてもよい。そのため、あらかじめ特定ユーザの音声パターン（例えば、声紋、ホルマント等）を記憶部７等に登録しておき、実際の音声認識動作時（例えば、図２のステップＳ２７）に、入力音声の特徴とそれらのパターンとを比較して、発声主が本人かどうかを判定するようにしてもよい。

【００８２】さらには、複数のキーワードとパスワードのペアの内、１組に対してのみ、特定ユーザの音声パターンを登録しておき、他の組については、不特定扱いとする構成をとってもよい。こうすることで、特定話者の音声認識のための構成が簡単化できる。なお、特定話者の音声認識技術は公知であるため、ここでは、その説明を省略する。

【００８３】このように、キーワードとペアになるパスワードとの同一性を音声的に照合するという処理と、特定の話者に対する音声認識という技術を組み合わせて、それらを端末機能として搭載することで、より一層、本人認識力を増強した携帯電話端末を提供できる。

【００８４】

【発明の効果】以上説明したように、第１の発明によれば、電子装置において、１対１に対応する１あるいはそれ以上のキーワードとパスワードの組を登録する手段と、これら登録されたキーワードとパスワードの組より任意のキーワードとパスワードを選択する手段と、上記選択したキーワードを表示する手段と、音声認識手段によって、当該電子装置外部からの音声を認識する手段と、上記認識結果をもとに、上記音声と、上記表示したキーワードと組になるパスワードとが一致するかどうかの照合処理をする手段とを備え、上記照合処理の結果、上記音声とパスワードとが一致した場合に、その音声の発声者を当該電子装置の使用者本人であると認証することで、使用者が煩雑なキー操作によるパスワード入力を行わずに、単純な手順で、高い秘匿性を持たせて、確実に使用者本人の認証を行うことができる。さらには、個人認識情報の事前登録なしに、簡単な構成で使用者本人の認証を行える。

【００８５】第１の発明に係る電子装置は、さらに、乱数を発生する手段を備え、その乱数に従って、上記登録されたキーワードとパスワードから任意の１組、あるいは複数組のキーワードとパスワードを選択することで、ランダムに現れるキーワードに対応したパスワードを用いた認証処理によって、パスワードの推測が困難となり、より安全性および秘匿性の高い、確実な本人認証を実現できる。

【００８６】すなわち、キーワードとパスワードの組の中から、乱数によってランダムに選択したキーワードとパスワードの組の全てについて同一性の照合処理を行うことで、第三者がパスワードを解読することが、より困難となり、厳密、かつ確実なユーザ認証を行えるという効果がある。

【００８７】また、第２の発明に係る本人認証方法によれば、１対１に対応する１あるいはそれ以上のキーワードとパスワードを登録するステップと、上記登録されたキーワードとパスワードの組より任意のキーワードとパスワードの組を選択するステップと、上記選択したキーワードを表示するステップと、電子装置の有する音声認識機能によって、その電子装置外部からの音声を認識するステップと、上記認識ステップで得た結果をもとに、上記音声と、上記表示したキーワードと組になるパスワードとが一致するかどうかの照合を行うステップと、上記照合ステップにおいて、上記音声とパスワードとが一致する照合結果が得られた場合、その音声の発声者を上記電子装置の使用者本人であると認証するステップとを備えることで、単純な手順で、確実に、かつ秘匿性を保持しながら電子装置の使用者本人の認証を行うことができる。

【００８８】また、第２の発明に係る本人認証方法は、さらに、乱数を発生するステップを備え、その乱数に従って、上記複数のキーワードとパスワードより任意の１組、あるいは複数組のキーワードとパスワードを選択することが、パスワードの推測を困難にし、結果として、より安全性、秘匿性の高い、高精度な本人認証を実現できる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係る携帯電話端末の主要部の構成を示すブロック図である。

【図２】実施の形態１に係る携帯電話端末における音声認識による本人認証動作および処理手順を示すフローチャートである。

【図３】記憶部に登録された複数組のキーワードとパスワードから１組を選択する様子を模式的に示す図である。

【図４】本発明の実施の形態２に係る携帯電話端末における音声認識による本人認証動作および処理手順を示すフローチャートである。

【図５】記憶部に登録された複数組のキーワードとパスワードからＮ組を選択する様子を模式的に示す図である。

【図６】携帯電話端末の動作と本人認証動作との関係を

示すフローチャートである。

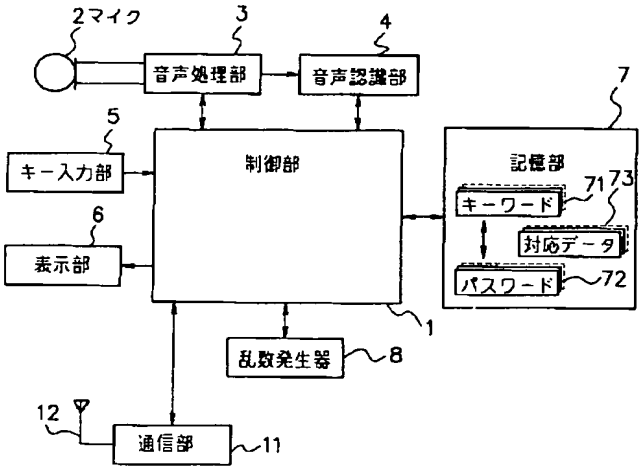
【図７】従来の通信機器の構成例を示すブロック図である。

【符号の説明】

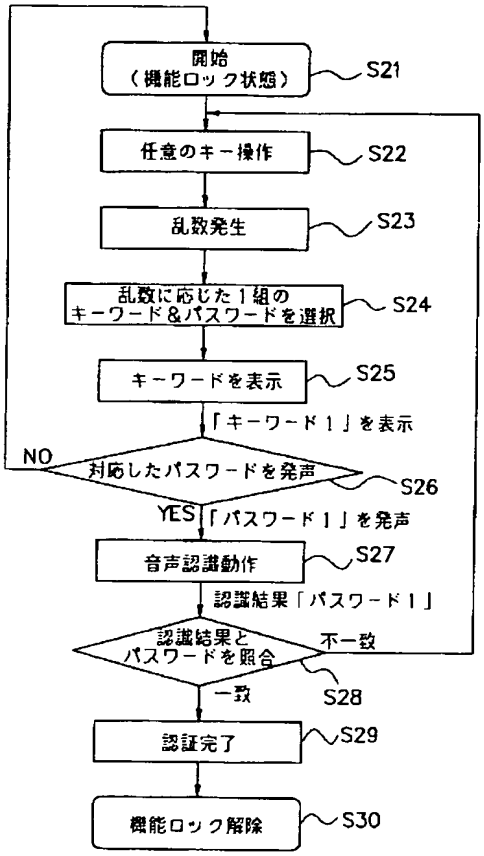
1　制御部
2　マイク
3　音声処理部
4　音声認識部
5　キー入力部

6　表示部
7　記憶部
8　乱数発生器
１１　通信部
１２　アンテナ
３１，５１，７１　キーワード
３２，５２，７２　パスワード
７３　対応データ

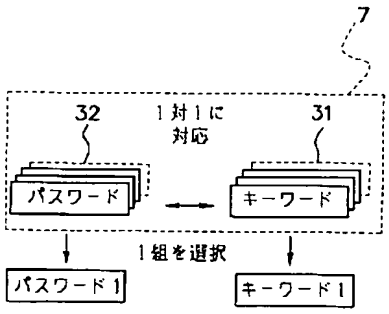
【図１】



【図２】

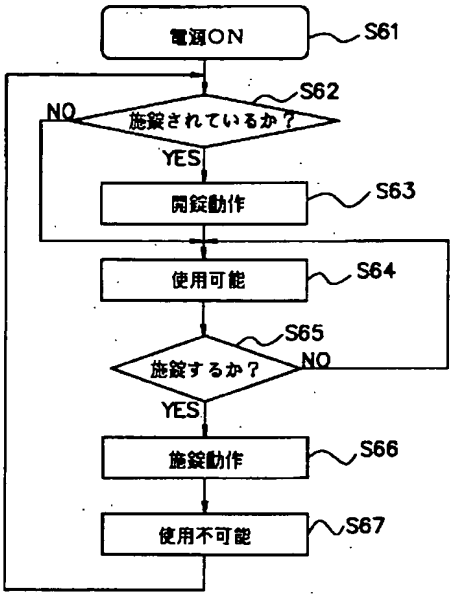


【図３】



【手続補正書】
【提出日】平成１４年６月１１日（２００２．６．１１）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００５４
【補正方法】変更
【補正内容】
【００５４】このようにキーワードとパスワードのペアを選択後、制御部１は、ステップＳ４６において、表示部６に、「キーワード１」～「キーワードＮ」の内、まず、「キーワード１」を、ユーザが認識できる文字形態で表示させる。そして、上記の実施の形態１の場合と同様に、ユーザが「キーワード１」の表示を見て、それに対応するパスワードの発声をするように促す。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図６
【補正方法】変更
【補正内容】

【図６】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｍ	1/00		Ｈ０４Ｍ	1/725	
	1/57		Ｇ１０Ｌ	3/00	５５１Ａ
	1/667				５７１Ｄ
	1/725				５４５Ｄ

Ｆターム(参考)　5B085 AE01 AE23 AE27 CE08
5D015 AA03 KK00 LL02
5K027 AA11 HH20 HH21
5K036 AA07 DD48 JJ02 JJ16 KK09